

REMARKS

Claims 1-22 are pending in the application. Claims 1-3, 9-11, 17-19, 21 and 22 stand rejected, and the balance of the claims stand objected to. Specifically, claims 4-8, 12-16 and 20 stand objected to for being dependent upon a rejected base claim but are indicated as allowable if rewritten into independent form. Applicant gratefully acknowledges the Examiner's provisional indication of allowability, but as fully explained in the following remarks, Applicant is of the opinion that all pending claims are in fact allowable over the art on record.

Rejection under 35 U.S.C §101

Claim 22 stands rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Applicant has hereby amended claim 22 to recite a computer readable storage medium and respectfully requests the Examiner to withdraw this rejection as moot in view of this amendment.

Rejection under 35 U.S.C §102

Claims 1-3, 9-11, 17-19, 21 and 22 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Published Patent Application No. 20040240666 to Cocks. With regard to claim 1, the Examiner essentially finds that Cocks discloses the entire claims at paragraphs 11-45 and 51-72 and in Figures 1 and 2. At the outset, Applicant protests the Examiner's rejection as incomplete and submits that the Examiner has failed to comply with the requirements of 37 C.F.R. §1.104(c)(2):

"In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by Applicant, **the particular part relied on must be designated as nearly as practicable.** The pertinence, if not apparent, must be clearly explained and each rejected claim specified" (emphasis added).

The Examiner does not discuss a single specific limitation of claim 1 nor point out the allegedly corresponding limitation in Cocks. Applicant is thus forced to guess at where each and

every claim limitation is allegedly disclosed by Cocks and then argue against his own guess, which Applicant submits is an onerous and improper burden for a patent Applicant to bear.

Nonetheless, in the interest of saving time and maximizing the period of protection afforded by an eventual patent, Applicant hereby submits a discussion of Cocks *vis a vis* his invention and make a good faith attempt at countering the Examiner's rejection.

Both the presently claimed invention and Cocks are in the field of so-called identifier-based encryption (henceforth "IBE"), the general precept of which is that data is encrypted using as encryption parameters (1) public data of a trusted authority (corresponding to the value N of the background discussion presented in the present application, more specifically at page 4, line 8), and (2) a public key string (the "encryption key string," see *e.g.* background discussion at page 4, line 24) that can be any arbitrary string but is often an identifier of the intended recipient. The thus-encrypted data is decrypted with a private key that is generated by the trusted authority using (a) the public key string and (b) private data of the trusted authority that is related to the public data of the trusted authority (the private data example in the background discussion is the two primes p and q the product of which gives N – see page 4, line 9). Knowledge of p and q is thus necessary to calculate the private key (as stated on page 5, line 18), while using the public data of the trusted authority as an encryption parameter ensures that only the trusted authority can generate the private key needed for decryption.

The present invention improves upon known IBE methods by using as the public key string, encrypted first data encrypted using an encryption key where the corresponding decryption key is held by the trusted authority (the trusted party corresponds to the first party of claim 1). Thus, when provided with the encryption key string, the trusted authority can not only generate the decryption key (for passing to the second party of claim 1), but can also recover the first data. Referring to the embodiment of Figure 4 solely for purposes of this discussion, the claimed "first data" corresponds to the payment details 43 that are encrypted by process 50 using a public key 40 of the trusted authority (the bank 35). The resulting encryption key string (EKS 44) is then used in process 51 to IBE encrypt an order form. The EKS 44 is passed to the bank 35 to generate the IBE decryption key 47 (by process 54) and to be decrypted (by process 53) to recover the payment details.

Cocks does bear a certain amount of similarity and thus relevance to the present application and it is in fact discussed at length in the present application (see page 3 lines 8-12, page 4 line 6 - page 6 line 6, and Figure 2). Indeed, the Quadratic Residuosity (QR) IBE method described in Cocks (and in Applicant's background discussion) is actually used within the embodiment of Fig. 3 of the present invention (see page 10, line 20). However, as clearly set forth in the specification, Cocks reveals but a subset of the method steps of the present invention.

Cocks' public key string (corresponding to Applicant's Encryption Key String) is limited to the identity of party A (ID_A), which is sent to the 'universal authority' U which then returns one of four possible roots 'r' – corresponding to the private key (the 'B' value in Applicant's description of the QR method). What Applicant's invention adds to the QR method described in Cocks is encryption of the identity ID_A before it is used in the QR method as well as the subsequent decryption of the encrypted ID_A by U. Applicant submits that neither of these steps is disclosed or suggested by Cocks and, given the lack of specific detail in the Examiner's rejection, it is difficult to submit any further argument.

Applicant's best guess is that the Examiner may consider Cocks' hashing of ID_A to correspond to the claimed encryption (see [0013] where ID_A is hashed to produce a quantity "a"). If this is indeed the case, Applicant respectfully disagrees, because such hashing is a conversion step that forms an essential part of any IBE method (see, *e.g.*, page 3 ll. 3-4 and Fig. 2 "EKS conversion," of the specification) and is not applied to produce an encryption parameter that is then used as input to the IBE encryption process; rather the hashing is part of the IBE process itself (please see, *e.g.*, present Fig. 2 at the top left). Furthermore, even if assuming for the sake of discussion that Cocks' hashing corresponds to the claimed encryption of the first data, there is no corresponding decryption effected by the trusted party (U of Cocks) as per claim 1 ("the first party uses a first decryption key to decrypt the encrypted first data, as provided to the first party in said third data, whereby to recover the first data," "the third data comprising the encrypted first data").

In view of all of the preceding, Applicant respectfully submits that claim 1 is in fact patentable over Cocks and, should the Examiner continue to disagree, Applicant respectfully

requests him to clearly and specifically point out where Cocks discloses each and every novel claimed feature discussed above in accordance with 37 C.F.R. 1.104(c)2.

Claims 9 and 17 stand rejected as being substantially equivalent to claim 1. Applicant therefore respectfully submits the claims 9 and 17 are allowable over Cocks for the same reasons set forth above with respect to claim 1.

Claims 2-3 depend from claim 1, claims 10-11 depend from claim 9, and claims 18-19 and 21 depend from claim 17. In view of the above discussion, it is submitted that claims 9 and 17 are allowable, and for this reason claims 2-3, 8-9, 18-19 and 21 are also allowable at least by virtue of their respective dependencies.

Applicant further submits that the above discussion regarding the allowability of claim 1 is equally probative of the allowability of claim 22, and respectfully requests the Examiner to pass this claims to issue as well.

Regarding the prior art made of record by the Examiner but not relied upon, Applicant believes that this art does not render the pending claims unpatentable.

In view of the above, Applicant submits that the application is now in condition for allowance and respectfully urges the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

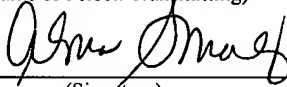
I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

April 11, 2007

(Date of Transmission)

Alma Smalling

(Name of Person Transmitting)

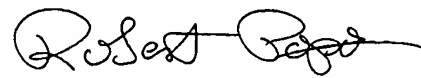


(Signature)

4/11/07

(Date)

Respectfully submitted,



Robert Popa

Attorney for Applicants

Reg. No. 43,010

LADAS & PARRY

5670 Wilshire Boulevard, Suite 2100

Los Angeles, California 90036

(323) 934-2300 voice

(323) 934-0202 facsimile

rpopa@ladasparry.com